



Endpoint Privilege Manager (EPM)

End User Guide

For  Mac &  Linux Users



Table of Contents

1. Introduction.....	03
2. How to Use the Securden Agent on Linux Devices?.....	03
3. How to Use the Securden Mac Agent?.....	04
4. How to Run Applications with Admin Rights?.....	04
5. How to Raise Requests for Permissions to Run Applications with Admin Rights?.....	06
6. How to Raise a Request for Temporary Local Admin Rights?.....	10
7. How to Raise Requests for Accessing Blocked Applications?.....	13
8. How to Run Commands with Sudo Privileges on Mac devices?.....	14

Securden Endpoint Privilege Manager

End User Guide – For Mac & Linux Users

Introduction

This guide is intended to be used by users working with Linux for command control and users working with Mac endpoints for gaining access to applications, elevating application privileges, and gain temporary admin rights using Securden Endpoint Privilege Manager.

Note: This document is designed to be used by all Linux users and Mac users without any admin rights. Typically, these users are a part of the 'Standard' group in their Mac device.

How to Use the Securden Agent on Linux Devices?



The Securden agent can be used to run certain commands with **sudo** privileges based on the control policy in effect.

1. If the administrator has granted sudo privileges for specific commands to the user, then the end user will be able to run these commands using the prefix sudo. For example, if the policy grants permissions to run the command 'apt update' with sudo permissions, the command will be executed as shown in the image below.

```
user@ubuntu:~$ sudo apt update
[sudo] password for user:
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2,345 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1,879 kB]
Fetched 4,560 kB in 2s (2,085 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

2. If the admin has denied sudo privileges for specific commands for this user, then the user would not be able to run the commands with sudo permissions. For example, if the policy denies permissions to run the command “apt update” with sudo for the user, the command will not be executed and the reason for not executing the command will be displayed as shown in the image below.

```
user@ubuntu:~$ sudo apt update
[sudo] password for user:
Sorry, user user is not allowed to execute '/usr/bin/apt update' as root on ubuntu.
```

How to Use the Securden Mac Agent?



Securden Agent provides provisions for standard users on Mac devices to gain temporary admin rights and elevate specific applications using Securden EPM.

The Securden Mac Agent can be used to perform the following operations:

1. Running Applications with Admin Rights
2. Raise Requests for Permission to Run Applications with Admin Rights
3. Raise Requests for Temporary Local Admin Rights
4. Raise Requests for Accessing Blocked Applications
5. Running Commands with SUDO Privileges

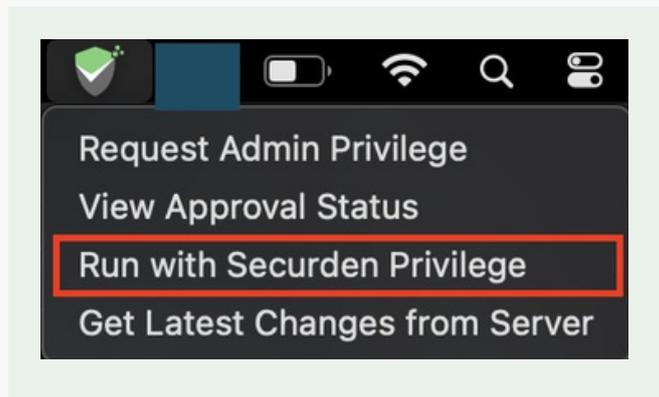
The steps involved in each of these operations have been explained in this document.

How to Run Applications with Admin Rights?

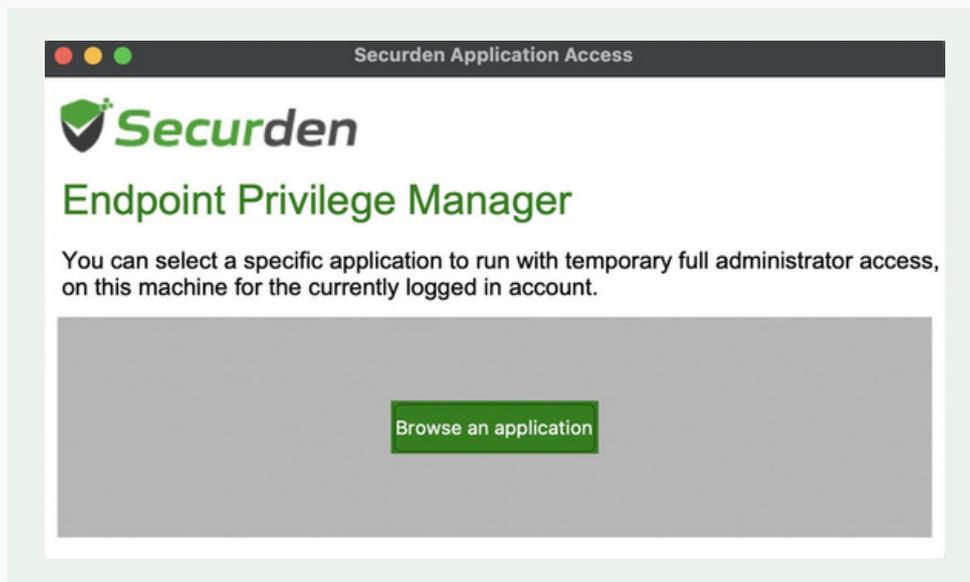


You can run applications with admin rights if you have the right permissions granted to you by an administrator. The EPM administrator can create policies that would allow you to run specific apps with admin rights on specific devices. If your admin has created one for you, you can run that specific app with admin rights by following the steps below.

1. Open the Securden Agent tray icon and select **Run with Securden Privilege**.



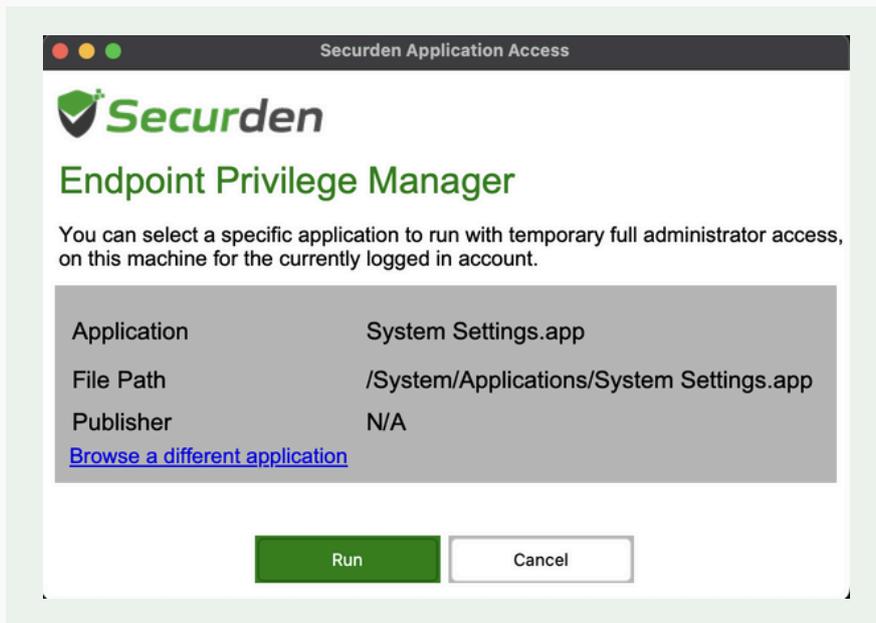
2. Click on **Browse Application**.



3. Navigate to the folder containing the application in Finder and select the required application.

Note: If the applications are greyed out (unclickable), you can click on **Show Options** and modify the filter to include **All Executables (*)**.

4. Once selected, click on Run in the dialog box that opens.



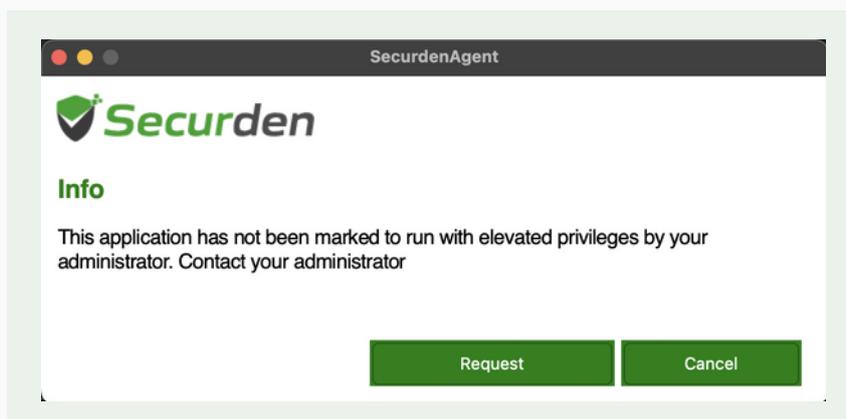
If your IT admin hasn't created a policy for you to be able to run a certain application with admin rights, the Securden agent will prompt you to place a request for permission to elevate the application.

This is explained further in the next section.

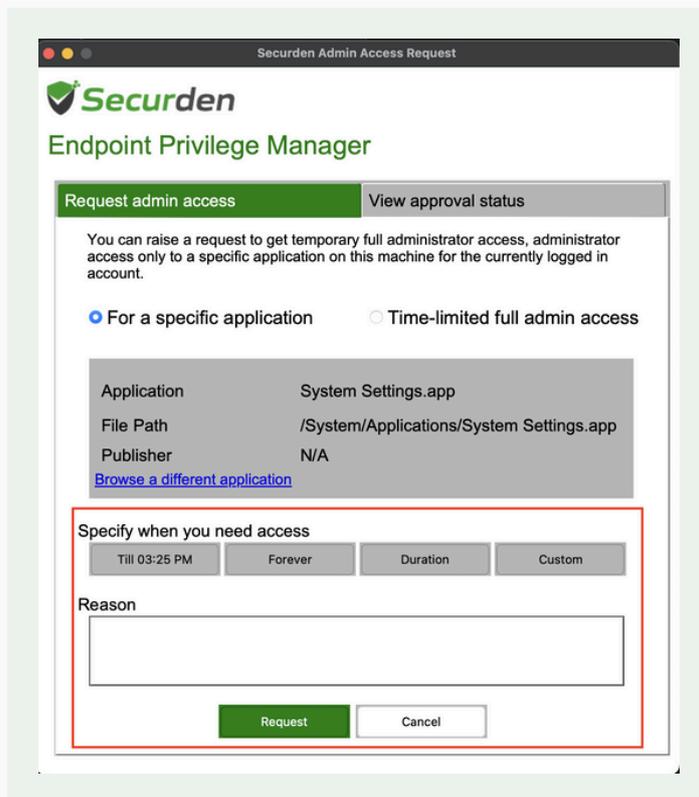
How to Raise Requests for Permissions to Run Applications with Admin Rights?



When you try to elevate an application, you do not have the permissions to elevate, the Securden Agent will prompt you to raise a request with the administrator. However, you can also use the Securden Agent tray icon to directly raise a request.

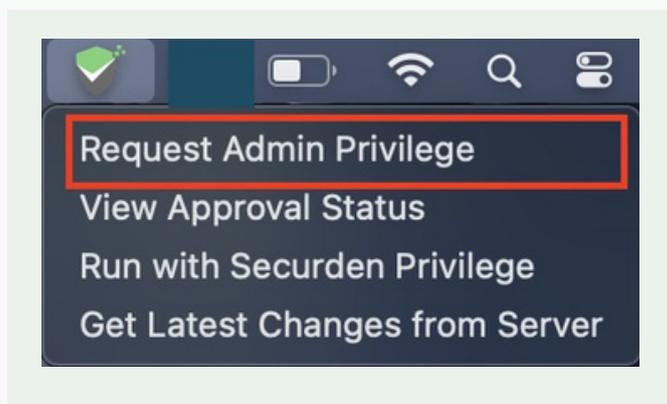


1. Click on Request.
2. Specify the time parameters of the elevated access. You have three options.
3. You can raise a request just by selecting the end time of access.
4. You can specify the duration of access without specifying the start time by clicking the Duration button.
5. If you want to specify both the start and end time of admin access, click on Custom and specify the time.

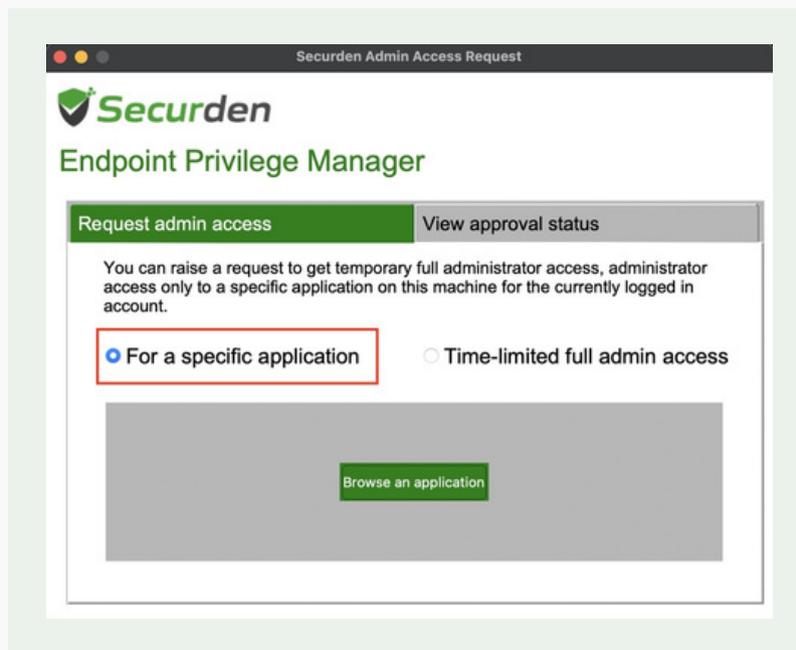


If you want to raise a request pre-emptively, you can use the Securden Agent tray icon to directly raise a request.

1. Open the Securden Agent icon and click on **Request Admin Privilege**.



2. Click on **For a Specific Application**.

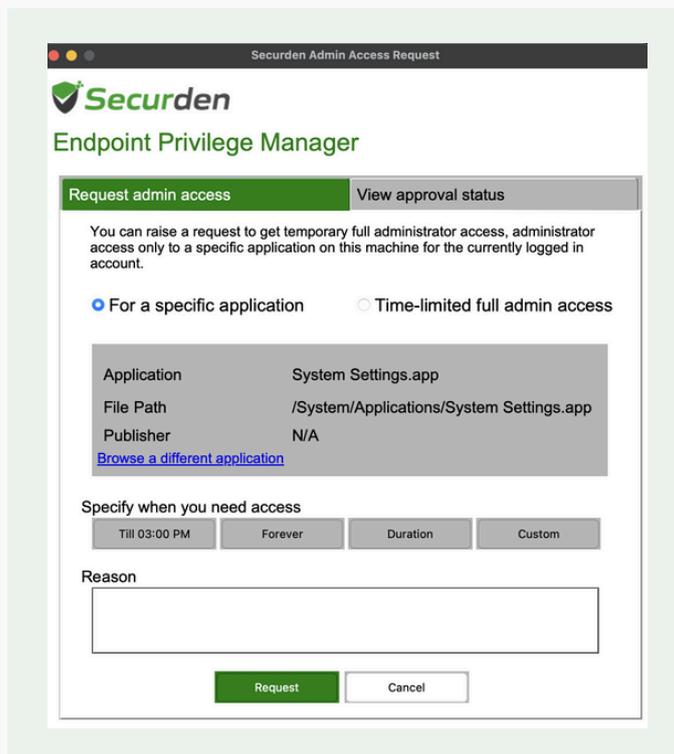


3. Click on **Browse an Application**. You will have to navigate through the files on your Mac and select the file for which you need elevated access permissions.

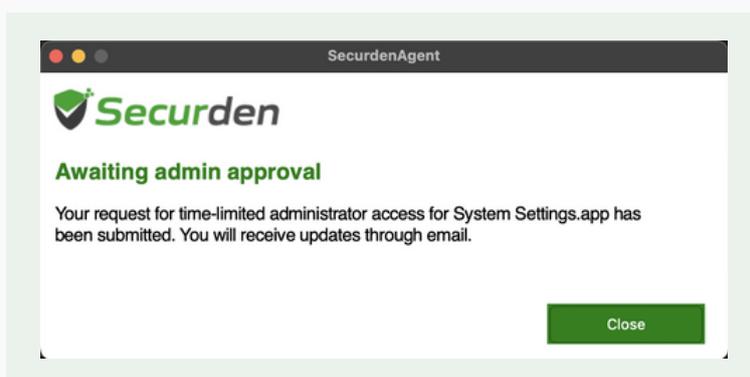
Note: If the applications are greyed out (unclickable), you can click on **Show Options** and modify the filter to include **All Executables (*)**.



- Once selected, you need to specify the start and end time of the elevated access. You can optionally place a request for a specific duration without specifying the start time.



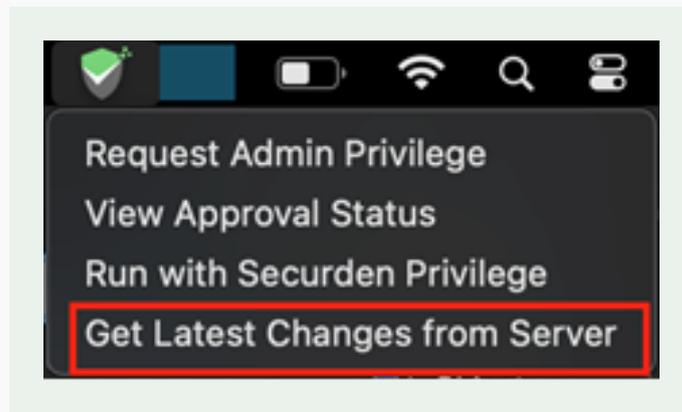
- Once the parameters are selected, state the reason for requesting elevated access and place the request.
- You will receive a confirmation message once the request is placed successfully.



Once the request is placed, the administrator or your designated approver will be alerted through email. Once they have approved the request, the user will be informed of the available access permission through email.

However, the agent communicates with the server only at fixed intervals. The agent might fetch the latest changes a few minutes after the admin approves the request.

If you want to manually fetch the latest changes from the EPM server, you can open the tray icon and click on Get Latest Changes from Server.



You can elevate the application by following the steps in the previous section.

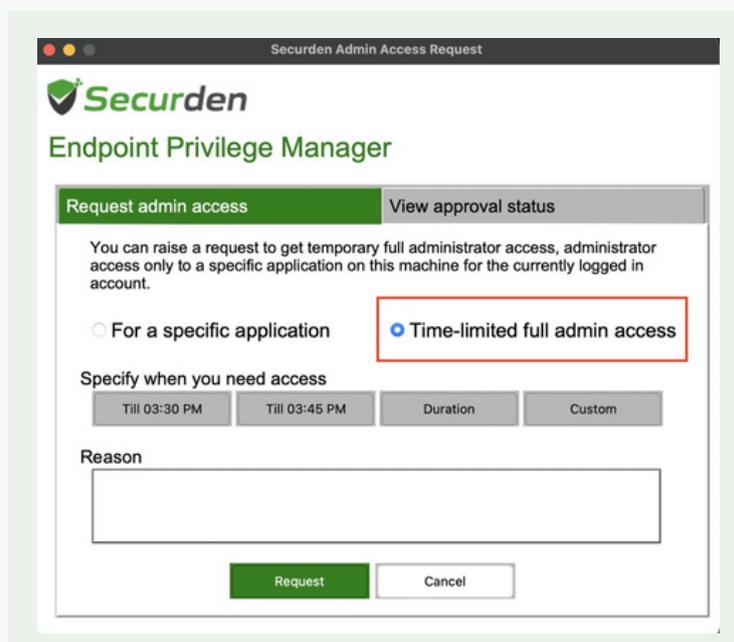
If you want to elevate multiple applications, you can raise a request for time limited local admin rights. This is discussed in the next section.

How to Raise a Request for Temporary Local Admin Rights?

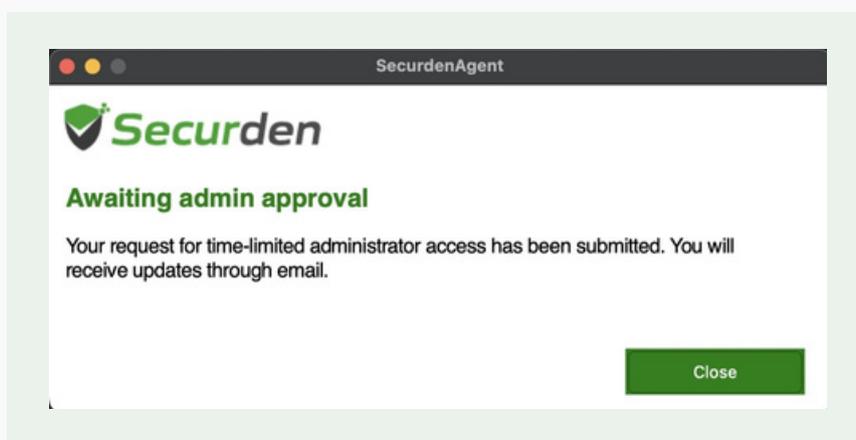


You can raise a request for temporary local admin rights using the Securden Agent. Open the tray icon and click on **Request Admin Privilege**.

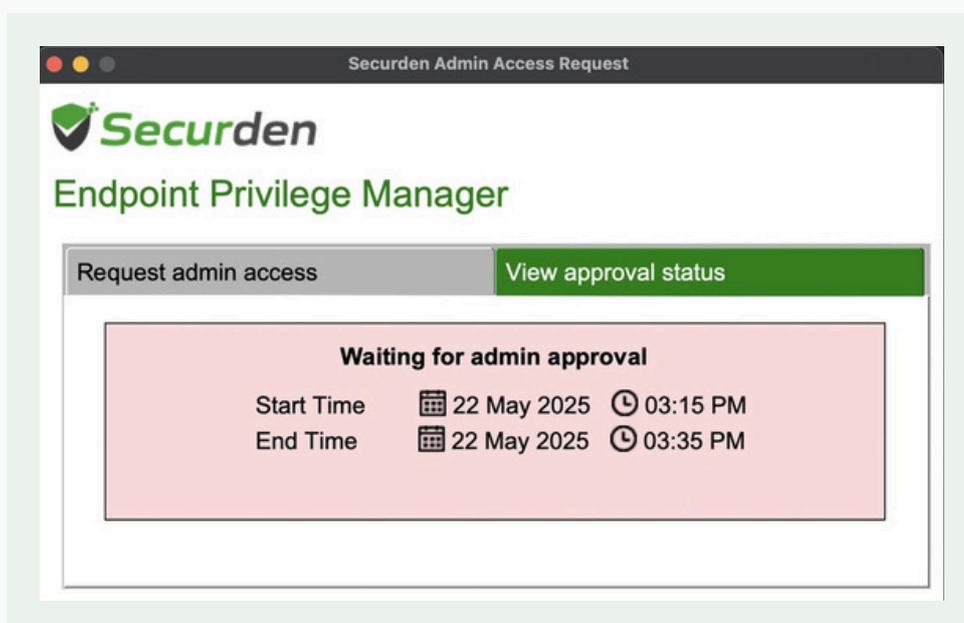
1. In the Agent pop-up, select **Time-limited full admin access**.



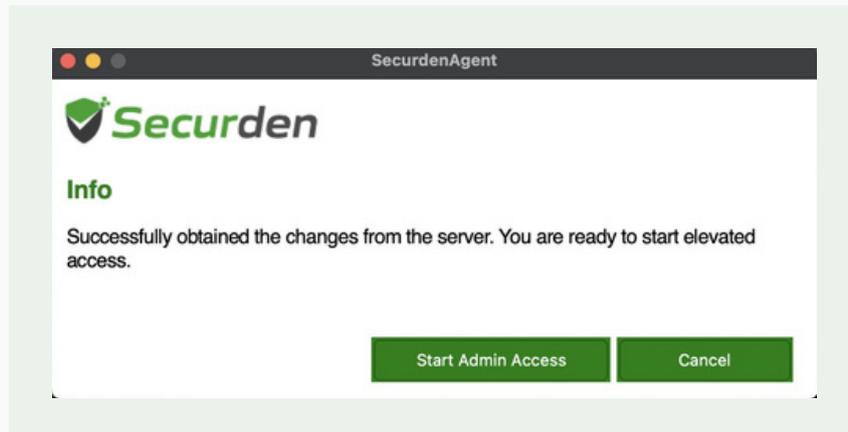
2. Specify the time parameters. You have three options.
 - a. You can raise a request just by selecting the end time of access.
 - b. You can specify the duration of access without specifying the start time by clicking the Duration button.
 - c. If you want to specify both the start and end time of admin access, click on Custom and specify the time.
3. Once the time parameters are selected, provide the reason for raising the request for local admin rights and click the Request button to place the request.
4. Once the request is raised, you will get a confirmation, and the administrator will be alerted.



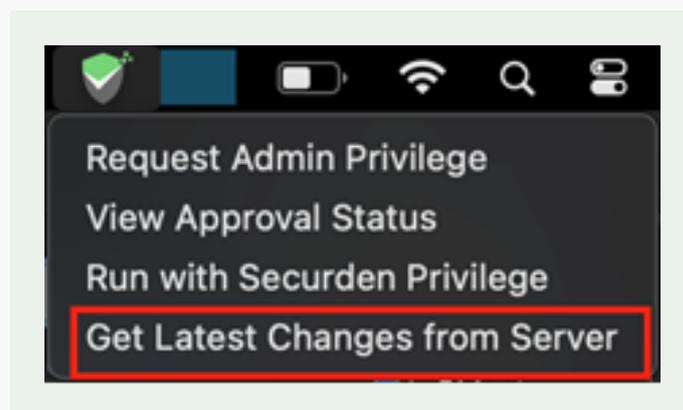
5. You can check the status of your requests by opening the tray icon and clicking on **View Approval Status**. A list of all your requests will be displayed along with the status.



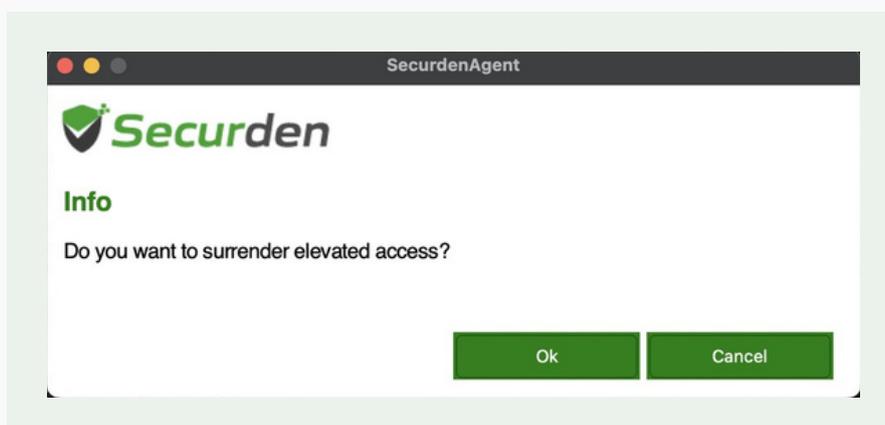
6. Once the administrator approves the request, the agent will alert you through a pop-up. You can start the local admin access by clicking on **Start Access**.



The agent will fetch the latest changes from the server at fixed intervals. However, you can manually fetch the latest changes by opening the Securden Agent Tray icon and clicking on **Get Latest Changes from Server**.



Note: Once you start your temporary access, a timer will be displayed in the bottom right corner. When the timer runs out, all open applications will be closed. You can manually surrender elevated access before the timer runs.

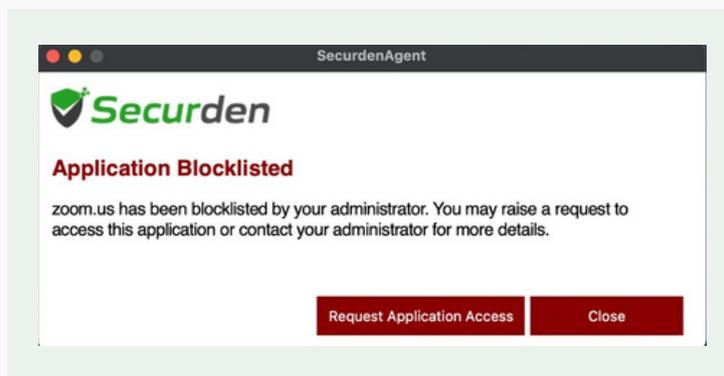


How to Raise Requests for Accessing Blocked Applications?

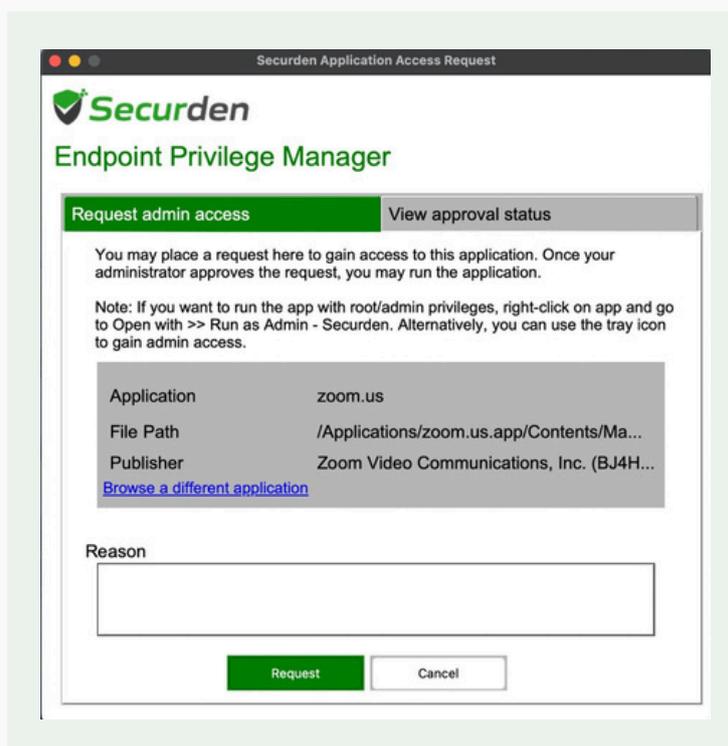


The EPM administrator can enforce application control by allowlisting and blocklisting applications through policies. If an allowlist or a blocklist is in effect, then you might not be able to access all applications on your Mac device. In such cases, you can place a request for application access using the Securden Agent.

1. The **Securden Agent** would automatically prompt you to raise an application access request when you try to run an application that hasn't been allowlisted for you.



2. When placing the request, you must provide a reason for requesting access before placing the request.



3. Once the administrator or your designated approver approves the request, you will be able to access the application. The agent communicates with the server in fixed intervals. You can manually fetch the latest changes by opening the agent icon and clicking on **Get Latest Changes from Server**.

How to Run Commands with Sudo Privileges on Mac devices?



The EPM administrator can create policies to allow specific users to run specific commands with SUDO privileges on specific endpoints. If you have one such command filtering policies associated with you, you can run the commands by appending the prefix sudo the command you want to execute.

```
user@MacBook-Pro ~ % sudo systemsetup -setremotelogin on
Password:
Remote Login: On
```

If you do not have **sudo** privileges, you will not be able to execute the command with the superuser privileges.